Anonymat et autonomie identitaire sur Internet

Davio, Etienne

Published in:
Droit des technologies de l'information : regards prospectifs

Publication date:
2000

Document Version
le PDF de l'éditeur

ANONYMAT ET AUTONOMIE IDENTITAIRE SUR INTERNET

Etienne DAVIO*

INTRODUCTION

La question de l'anonymat sur Internet apparaît comme un thème particulièrement controversé et autour duquel les passions se déchaînent. De façon caricaturale, deux clans se font face. Les uns voient dans l'anonymat l'ultime rempart de la liberté et de la vie privée ; l'anonymat constitue un instrument de survie de l'espèce. Les autres redoutent l'anarchie et l'incivisme. L'anonymat entraînerait la perte de l'identité, fondement discret de notre organisation sociale.

Le présent article se propose de mettre en lumière les termes de ce débat. Il ne s'agira pas de trancher à chaud, sur le mode du pour au contre, mais au contraire de proposer les outils d'une analyse nuancée. L'espoir est d'amener le débat sur la scène juridique et de stimuler une réflexion sur l'anonymat qui semble, à ce jour, particulièrement discrète dans les droits européens[1].

La première section s'attachera à clarifier le sens même de la notion d'anonymat et la place qu'elle occupe, dès à présent, dans l'organisation juridique, afin d'inscrire notre réflexion dans le cadre existant. Les juristes n'ont, en effet, pas attendu le *world wide web* pour envisager différentes situations de dissimulation de l'identité.

Dans la deuxième section, l'accent sera mis sur les technologies utilisées sur Internet afin d'assurer une maîtrise plus ou moins élargie des données identitaires personnelles. Il s'agira de rendre compte des subtiles déclinaisons du concept d'anonymat présentes sur le réseau.

La conclusion s'efforcera de confronter les données juridiques et techniques afin de donner à la question de l'anonymat sa portée véritable. Il

---

* Maître de conférences aux FUNDP.

1 Dans la littérature récente, on notera l'article de J. POUSSON-PETIT, « Le droit à l'anonymat », *Mélanges dédiés à Louis Boyer*, Toulouse, Université des Sciences Sociales, 1996, pp. 596-621. La question est nettement plus débattue dans les droits nord-américains, en particulier, dans le contexte du cyberespace. Voy. par exemple Anne BRANSCOMB, Anonymity, Autonomy and Accountability: Challenges to the First Amendment in Cyberspace, 104 *Yale L.J.* 1639 (1995); George P. LONG, III, Note, Who Are You ? Identity and Anonymity in Cyberspace, 55 *U. Pitt. L. Rev.* 1177 (1994); M. FROOMKIN, « Anonymity and its enmities », 1995 *J. Online L.* art. 4, accessible à l'adresse http://www.law.cornell.edu/jol/froomkin.htm.

s'agira, pour l'essentiel, de dénoncer l'identification massive qui s'est développée au fil des ans.

SECTION 1. L'ANONYMAT ET LE DROIT

§1. Identification et anonymat en droit

Il serait faux de penser que la question de l'anonymat n'a vu le jour en droit qu'avec l'avènement des nouvelles technologies de l'information et de la communication. De longue date, le droit intervient pour protéger, imposer, tolérer, interdire voire imposer l'anonymat[2].

Cette diversité d'attitude témoigne de la multiplicité des contextes dans lesquels la question de l'anonymat est posée. Le paragraphe 3 de la présente section proposera une classification de ces différents contextes.

L'existence d'une réflexion juridique sur ce thème est le fruit de l'omniprésence de la notion d'identification dans notre organisation juridique[3]. Le processus d'identification, dont on retrouve un grand nombre de manifestation en droit, couvre un très large spectre, tant sous l'angle des finalités (quand et pourquoi identifie-t-on ?) (1°), que sous l'angle des modalités (comment identifie-t-on ?)(2°).

(1°) Sans pouvoir entrer dans le détail, force est de constater que bon nombre de nos interactions sont réalisées en faisant référence à notre identité. Cela est particulièrement vrai en matière de communication : on peut affirmer que tout échange d'informations inscrit dans la durée va, à un stade ou un autre, aborder la question de la reconnaissance ou de l'identification de l'interlocuteur. Ainsi en est-il d'une carte postale, d'une communication téléphonique, d'un contrat[4], de l'expression d'une opinion politique. Dans les relations humaines semble prévaloir un principe général d'identifiabilité, que le droit a, pour l'essentiel, fait sien. Cela dit, le droit n'est intervenu que dans un nombre limité de cas pour formaliser le processus d'identification : on pense par exemple aux documents d'identité, aux règles entourant les contrôles d'identité, à l'exigence de signature manuscrite dans les actes sous seing privé.

---

2 J. POUSSON-PETIT, *op. cit.*, p. 597.

3 L'identification se définit comme l'action d'identifier. Sous l'angle juridique, il s'agira essentiellement, de reconnaître une personne sous l'angle de l'état civil.

4 Le contrat instantané semble déroger à la nécessaire identifiabilité. En l'occurrence, il ne s'agit pas d'un échange d'informations inscrit dans la durée. Cela dit, l'anonymat (relatif) ne concerne, en général, qu'une seule des deux parties, l'acheteur dans l'hypothèse d'une vente.

(2°) Les modalités de l'identification sont extrêmement diversifiées. En fonction du contexte, les intervenants adopteront des attitudes très diverses, préconisant tantôt une identification hautement formalisée, tantôt une identification incidente. À l'extrême de cet éventail de stratégies identitaires[5], certains acteurs vont parfois rechercher l'anonymat en évitant toute communication d'informations identitaires.

§ 2. L'anonymat comme mise en péril de l'obligation de rendre compte

Si l'anonymat est problématique en droit c'est qu'il met en cause le principe essentiel selon lequel on doit rendre compte de ses actes, tant sur le plan civil que pénal. Cette *obligation de rendre compte* que les auteurs anglo-saxons désignent par la notion d'*accountability*, peut être définie comme l'acceptation des responsabilités découlant de ses actes.

La mise en œuvre de *l'obligation de rendre compte* va directement reposer sur l'identification de son sujet passif. On pense, par exemple, à la signature apposée au bas d'un contrat, au numéro d'immatriculation qui permet de retrouver l'auteur d'un accident de circulation, au relevé d'empreintes digitales qui permettra une inculpation. Une identification du débiteur ou du fautif est indispensable. L'anonymat vient l'empêcher[6].

La perte d'imputabilité qu'engendre l'anonymat constitue un cuisant revers pour un système tout entier dédié au rattachement de droits et d'obligations à des personnes déterminées. Dans un tel contexte, l'anonymat, source de dilution de la responsabilité[7], ne peut être qu'exceptionnel, l'identifiabilité constituant un impératif implicite de la technique des obligations.

Cela dit, l'existence de situations diversifiées dans lesquelles l'anonymat va être admis, en droit, témoigne d'une marge de négociation sur le terrain de l'identifiabilité. Dans chacun des cas où l'anonymat est consacré, l'identifiabilité cède du terrain face à un intérêt supérieur.

---

5 L'expression est de C. CAMILLERI et *alii*, *Stratégies identitaires*, Paris, Puf, 1990.

6 A. BRANSCOMB, o*p. cit*, p. 1645.

7 J. Kastersztein, «Les finalités identitaires des acteurs sociaux: approche dynamique des finalités», in C. CAMILLERI et *alii*, *op. cit.*, pp. 34-35. J. Kasterzstein met le doigt sur un aspect intéressant: l'anonymat fonctionnerait comme un facteur déresponsabilisant et, simultanément, comme un révélateur des potentialités individuelles. Ainsi , lors d'une interrogation en condition anonymante les écarts entre élèves sont plus faibles que si l'identité de chacun a été révélée. « Tout se passe comme si dans le mode d'insertion anonymant la pression sociale était plus faible et que les conduites de cohérence sociale des élèves ne jouaient plus ».

§3. Les agissements anonymes

1. Anonymat passif et anonymat actif

L'anonymat vise l'état de la personne dont on ignore le nom ou qui ne fait pas connaître son nom[8]. L'anonymat peut découler de deux attitudes: tout d'abord, une attitude passive qui consiste à rester à l'écart des interactions sociales pour éviter de faire l'objet d'identifications. Dans cette acception, le droit à l'anonymat constitue un des aspects de la protection de la vie privée : le droit d'être laissé tranquille.

Le droit de vivre anonyme signifie en pareil cas le droit de vivre à l'abri de toute intrusion. Madame Pousson y voit là un aspect fondamental du droit à l'anonymat qu'il convient de privilégier. S'il apparaît clairement que ce droit à l'intimité est un élément central de la *privacy*, il nous semble inadéquat de privilégier l'appellation « droit à l'anonymat », pour décrire cette facette de la vie privée: ce n'est pas la question de l'identité, envisagée au travers de la diffusion du nom ou d'identifiants qui est en cause. Ce qui prime c'est la tranquillité. Tout au plus en découle un anonymat passif, qui n'apparaît pas comme une modalité spécifique de l'action humaine, mais comme le résultat d'une mise à l'écart de la société. L'actrice qui se détend aux abords d'une piscine, cherche, non pas à rester anonyme, mais à ne pas être la cible des photographes. Évidemment, si son absence dans les médias se prolonge, elle sombrera dans « l'anonymat » le plus total[9].

L'anonymat peut également être recherché activement : il devient un anonymat dans l'action qui consiste à ne pas être identifié alors qu'on agi.[10]. Dans ce deuxième sens, l'anonymat constitue une modalité tout à fait particulière de l'action humaine, en ce qu'il coupe court aux identifications attendues. Cet anonymat actif est de nature à jouer un rôle particulièrement sensible dans les processus de communication, ainsi qu'en témoigne l'importance prise par cette question dans le réseau Internet. Notre étude s'attachera à cette face active de l'anonymat dont on trouve différents échos en droit.

---

8 Dictionnaire le petit Robert, 1998.

9 Cette dimension passive de l'anonymat peut encore prendre un tour involontaire: ainsi on déplorera l'anonymat qui règne dans les grandes villes.

10 Dans cette optique, on peut retenir la définition suivante « Anonymity can refer to a person's failure to « sign » speech or action, in the sense of deliberately revealing herself in a conventional manner as having made or done it »: L. TIEN, « Who's afraid of anonymous speech ? *McIntyre* and the Internet , *Oregon Law Review*, vol. 75, n° 1, 1996, p. 159.

2. Méthodes de l'anonymat actif

L'anonymat procède par l'effacement ou l'omission des données identifiantes. Ces données sont nombreuses. Il s'agit, d'une part, des données de l'identité civile : le nom, le domicile, auxquelles viennent s'ajouter de nouveaux outils d'identification sous forme d'identifiants codés (numéro de la sécurité sociale, numéro d'immatriculation du véhicule, numéro de téléphone, numéro de la carte de crédit). Il s'agit, d'autre part, des données de l'identité physique : l'apparence physique, le visage, la voix, les empreintes digitales ou génétiques,...[11] Il peut encore s'agir d'un comportement spécifique, permettant de reconnaître une personne : ainsi, est annulé le vote du conseil communal dont un des membres a utilisé un bic à l'encre verte : l'anonymat des votes exprimés n'est plus assuré[12].

En première analyse, on peut considérer que constitue une donnée identifiante tout élément permettant d'atteindre une personne déterminée, dans son contexte physique[13]. On parlera dans cette hypothèse d'une identification traditionnelle. Dans ce cas, la donnée identifiante, le nom par exemple, fait office de passerelle en direction d'une personne.

L'examen des éléments apparaissant comme identifiants lors de la communication sur Internet conduit à proposer un élargissement des données qualifiées d'identifiantes aux données permettant, seulement, une identification innovante: elles ne permettent pas de retrouver la personne dans son contexte physique, mais offrent un point d'ancrage, un point d'amalgame permettant d'agréger l'ensemble des informations relatives à une personne. (Sur cette distinction, *cf. infra* Section 2, §1)

3. Les multiples visages de l'anonymat actif

À ce stade, un double constat s'impose : tout d'abord, celui de la rareté des études consacrées à la question de l'anonymat et, ensuite, celui de l'extrême difficulté d'une réflexion d'ordre général sur le sujet[14]. Cette double réalité s'explique : au-delà du mot *anonymat*, on découvre un grand nombre de situations disparates.

Il convient d'opérer une classification des situations dans lesquelles l'anonymat est revendiqué, et ce, en fonction des finalités poursuivies. Il

11 J. POUSSON-PETIT, *op.cit.*, p. 602.

12 C.E. n° 38.062, 6 novembre 1991, *R.A.C.E.*, 1991.

13 Il s'agit soit de pouvoir retrouver cette personne, soit de la localiser à son domicile.

14 L'étude de Madame POUSSON-PETIT précitée apparaît comme une des seules contributions directement consacrées à ce thème.

apparaît que les situations dans lesquelles l'anonymat se manifeste peuvent être rangées en quatre catégories[15].

1° L'anonymat de l'auteur de certains faits juridiques

L'anonymat de l'auteur de certains faits juridiques est consacré dans différentes situations, afin de permettre à l'auteur d'échapper à certaines conséquences de son acte. Il s'agit ici d'un anonymat spécial, en ce sens qu'il résulte d'une norme juridique spécifique.

Les illustrations les plus nombreuses figurent dans le droit de la famille, en particulier en matière de filiation : on pense évidemment à l'accouchement sous X, reconnu en France par l'article 341-1 de la loi du 8 janvier 1993[16]. Toujours dans ce domaine, l'anonymat du donneur de gamètes est instauré dans diverses législations[17]. On trouve également trace de l'anonymat, à titre exceptionnel, dans le procès pénal. Ainsi en est-il des dispositions visant à assurer l'anonymat des informateurs, des agents infiltrés et de certains témoins[18].

Sous l'angle des finalités, il s'agira pour la mère qui a accouché sous X de ne pas avoir à assumer la maternité et les obligations qui s'y rattachent. On vise à permettre l'accouchement et l'abandon par préférence à un avortement clandestin. L'objectif est de protéger la mère, la vie de l'enfant et de favoriser l'adoption[19]. Pour le témoin, il s'agira de ne pas s'exposer à des représailles en raison des révélations qu'il aurait faites ; on vise à permettre un témoignage par préférence au règne de la loi du silence.

Ce traitement disparate conduit à consacrer, en droit, un anonymat de circonstance obéissant à des objectifs, modalités et sanctions propres. Il s'agit là d'entorses mineures, jugées nécessaires, à un principe général d'identifiabilité des agents juridiques évoqué précédemment.

L'anonymat vient heurter les intérêts de ceux qui souhaitent la révélation de l'identité. Ainsi sur le terrain de la filiation, l'anonymat reconnu aux géniteurs coupe court à toute possibilité pour l'enfant de connaître, un jour, ses origines biologiques. La reconnaissance progressive d'un droit pour l'enfant à connaître le secret de ses origines vient lézarder le mur du silence qu'engendre l'anonymat. En France, des voix s'élèvent pour qu'à l'anonymat total et définitif soit substitué un système reposant

---

15 Ce classement est certes arbitraire ; des chevauchements ne tardent d'ailleurs pas à voir le jour. Il permet néanmoins une clarification du débat.

16 Cl. NEIRINCK, « L'accouchement sous X: le fait et le droit », *J.C.P.*, 1996, I, 3922.

17 A. ROUVROY, «Quelques questions relatives aux procréations médicalement assistées», *J.T.*, 1997, pp. 769-777.

18 J. de HEMPTINNE, « La déposition de témoins sous anonymat devant le tribunal pénal international pour l'ex-Yougoslavie », *J.T.*, 1998, pp. 65-69.

19 J. POUSSON-PETIT, *op. cit.*, p. 607.

sur le secret, relatif par essence, lequel pourrait être levé dans des circonstances clairement définies.

À ce stade, l'anonymat apparaît bel et bien comme « une institution pour temps de crise »[20]. Il est retenu dans des situations exceptionnelles et vise à assurer la sauvegarde immédiate d'un intérêt gravement menacé.

2° L'anonymat pour assurer la sauvegarde des intérêts des parties au contrat

À nouveau l'anonymat est cantonné à des situations spécifiques. Certains mécanismes du droit des contrats permettent la dissimulation de l'identité tantôt à l'égard du cocontractant (il s'agit d'éviter que la prise en compte de l'identité influence le cocontractant), tantôt à l'égard des tiers (les motivations sont diverses : volonté de fraude, de discrétion, de protection de la vie privée).

Dans le premier cas, il s'agira souvent d'un anonymat temporaire cantonné à l'époque de conclusion du contrat. Le mécanisme de déclaration de command ou celui du prête-nom permettent de préserver l'anonymat d'un contractant. L'objectif est d'éviter que la révélation de l'identité puisse compromettre la conclusion du contrat. Ces mécanismes permettent de concilier la non-révélation de l'identité du contractant et le respect des engagements pris par ce dernier.

Cela dit « l'anonymat ne pénètre que difficilement le cercle contractuel fondé essentiellement sur des relations personnelles de confiance »[21]. Si le recours à ces mécanismes reste relativement rare, il témoigne que l'anonymat n'est pas incompatible avec le respect des engagements de celui qui contracte.

Dans le second cas, l'anonymat est utilisé pour échapper à l'emprise des tiers sur le contrat. Tel est le cas du recours à un paiement en liquide. Il s'agit bien plus, en fait, d'assurer la confidentialité du contrat que de rechercher l'anonymat. On notera le recul manifeste de l'anonymat, dans de nombreux contrats instantanés, en raison du recours à des moyens de paiement identifiants, qui formalisent et archivent ces opérations. Le groupe 29, créé par la directive européenne sur la protection des données, préconise le droit de pouvoir recourir à des moyens de paiement anonymes.

---

20 L'expression est du professeur J.-P. DESCHANEL qui constate l'existence d'opérations bancaires anonymes : le change manuel, le rapatriement d'avoirs à l'étranger, les transactions sur l'or, la souscription de bons, *in* « Les opérations bancaires peuvent-elles être anonymes ? », *Annales de la Faculté de droit et de sciences politiques*, Université de Clermont I, 1988, p. 1 cité par J. POUSSON-PETIT, *op. cit.*, p. 597.

21 J. POUSSON-PETIT, *op. cit.*, p. 597.

3° L'anonymat pour assurer la liberté d'expression

Tel que décrit jusqu'à présent, l'anonymat, lorsqu'il était consacré ne l'était qu'à titre exceptionnel. Mise au service de valeurs beaucoup plus larges — la liberté d'expression, la vie privée — la perception du concept va changer du tout au tout.

Une facette fondamentale consiste à en faire un instrument au service de la liberté d'expression. Partant du constat que l'identification peut avoir pour effet de brider la libre expression et conscient que des opinions novatrices et salutaires n'auraient jamais vu le jour si leur auteur n'avait pu se préserver en passant sous silence son identité, on en arrive à considérer la nécessité de reconnaître un droit à l'anonymat, en particulier dans la relation à l'autorité.

La jurisprudence américaine a consacré ce droit dans diverses affaires, dont le célèbre arrêt Mc Intyre. Par cet arrêt, la Cour suprême a sanctionné une législation de l'Ohio au motif qu'elle prohibait, de façon générale, le recours à l'anonymat à l'occasion d'un discours politique. La Cour a considéré que la décision de rester anonyme ou non relevait de l'autonomie de la personne qui s'exprime et que cette décision relevait du contenu même de la publication, et qu'à ce titre elle était protégée par le premier amendement[22].

Cette jurisprudence ne revient pas à consacrer un droit à l'anonymat généralisé, mais plutôt de faire de ce dernier l'une des modalités possibles de la liberté d'expression. Différents auteurs se sont penchés sur la transposabilité de cette jurisprudence au cyberespace[23]. À dire vrai, il semble tout à fait naturel que cette jurisprudence puisse trouver à s'appliquer quelque soit le médium utilisé : il conviendra à chaque fois de composer avec les caractéristiques techniques du moyen de communication utilisé.

Dans les droits continentaux, le droit à l'anonymat est surtout envisagé dans son aspect passif[24]. Sur le terrain de l'anonymat actif, il n'existe apparemment pas de consécration équivalente à celle contenue dans la jurisprudence américaine. On peut signaler, toutefois, que le droit au silence qui « par rapport à la liberté d'expression, … signifie le droit d'être maître de sa communication avec autrui »[25] apparaît comme une consécration indirecte du droit à rester anonyme.

---

22 *McIntyre*, 115 S. Ct. At 1514. Pour un commentaire de la décision, voy. L. TIEN, *op. cit.*, pp. 123-125.

23 L. TIEN, *op. cit.*, pp. 117-189. G.H. Carr, « Application of U.S. Supreme Court doctrine to anonymity in the net world », *Cleveland State Law Review*, Vol 44 (1996), pp. 521-548.

24 J. POUSSON-PETIT, *op. cit.*, p. 598.

25 L.-E. PETTITI, « Introduction », *Le droit au silence et la détention provisoire*, Bruxelles, Bruylant, 1997, p. 7.

4° L'anonymat comme rempart de la vie privée

Si l'identification sert de clé à la mise en œuvre de l'obligation de rendre compte de ses actes, force est de constater qu'elle va, également, servir de sésame à la collecte d'informations personnelles.

En raison de l'efflorescence des instruments de collectes et de traitement des données personnelles, un anonymat actif est de plus en plus souvent revendiqué afin de couper court à la collecte de semblables données. La non-communication de données identifiantes apparaît, en somme, comme l'ultime rempart de la vie privée : seule l'opacité des identifiants peut assurer à l'Internaute d'être laissé en paix[26].

Si la stratégie identitaire revendiquée par les Internautes, et qui vise une extension majeure de l'anonymat, obéit à une certaine logique de raisonnement, il s'impose de la confronter à la réalité technique du réseau. La question qu'il convient de se poser est, alors, de savoir comment l'anonymat peut être atteint sur Internet (Section 2) ?

SECTION 2. LA TOILE MYSTÉRIEUSE : LES TECHNIQUES DE L'ANONYMAT SUR INTERNET

L'anonymat tel qu'il est recherché sur Internet poursuit trois ordres de finalités : assurer l'anonymat des opérations contractuelles, permettre la libre expression, empêcher les intrusions dans la vie privée. La particularité du débat sur l'anonymat sur Internet est qu'il s'inscrit en totalité dans un environnement technologique : cette problématique est indissociable des méthodes de connexion et de communication mises en œuvre.

La technique utilisée implique de nombreuses identifications, que l'anonymat tentera de contrer. Dans cette optique, il convient de commencer par l'étude des procédés d'identification sur Internet (§1), pour ensuite aborder les procédés d'anonymisation (§2).

§ 1. La technique et l'identification

Dès le moment où une technique soutient le processus de communication, elle façonne le déroulement de l'identification. Jusqu'il y a peu, la technique sous-tendant une communication téléphonique n'offrait à l'appelé aucun moyen d'identification de l'appelant. C'est seulement au stade de la conversation téléphonique qu'intervenait, ou non, l'identification. Aujourd'hui, la communication du numéro de l'appelant

26 Y. POULLET, « Libertés et société de l'information: le droit de participer à la société de l'information et le droit de s'en exclure », *Revue Ubiquité*, 1998, liv. 1, pp. 21-27. Le droit à l'anonymat semble concilier l'alternative du titre : il offrirait de pouvoir prendre part à la société de l'information tout en s'en protégeant.

est en passe de se généraliser. Sur Internet, en l'absence d'opérateur, la technique de communication procure au destinataire de la communication des informations sur l'expéditeur ou sur l'ordinateur qu'il utilise.

Dans le premier cas, la perte d'anonymat que représente la communication du numéro de téléphone de l'appelant est analysée avec une inquiétude certaine[27]. Sur Internet, l'anonymat paraît aller à contre-courant des identifications omniprésentes, et dès lors, est pris pour cible.

1. L'identification sur Internet

1° Identification active et passive

L'identification peut revêtir deux aspects : une distinction peut-être établie entre identification active, qui suppose une démarche spécifique de l'internaute visant à permettre son identification, et identification passive, qui vise l'identifiabilité résultant de la seule technique de communication utilisée. Par identification active, on vise essentiellement le recours à un mécanisme de signature au moyen duquel l'auteur d'un message offre un signe vérifiable de son identité. Cette question ne sera pas abordée dans cet article. L'autre facette vise l'identification passive : la mise en œuvre de la communication présuppose la communication de données permettant une identification.

2° Identification traditionnelle et innovante

Traditionnellement, l'identité est entendue en dernier ressort comme celle d'une personne physique déterminée. Les éléments qui servent à individualiser une personne physique, pour l'essentiel les éléments de l'état civil, permettent de renforcer l'appréhension d'un individu dans son contexte physique. Les données de l'identité civile et de l'identité physique se complètent et interagissent. Elles se rapportent à un socle commun : une personne physique déterminée. Lorsque l'identification opérée permet de retrouver, physiquement, une personne, on considérera qu'il y a identification traditionnelle.

Sur Internet, on retrouve également des données identifiantes qui vont permettre une identification traditionnelle: lorsqu'un hacker est localisé et arrêté sur base d'informations qu'il a involontairement fournies aux réseaux, c'est une personne physique déterminée qui est retrouvée. De même lorsque l'adresse de courrier électronique contient des noms et prénoms c'est à nouveau une personne physique qui est désignée. L'identification traditionnelle est celle qui permet d'isoler, dans son contexte physique, un individu des autres.

---

27 C. BOURGEOS, « La «présentation du numéro » : un nouveau recul de l'anonymat ? », *D.I.T.*, 1998/2, pp. 84-86.

Une nouvelle forme d'identification apparaît sur Internet, comme conséquence des innovations technologiques. L'identification d'une personne s'opère sans référence aux éléments classiques d'identification, à savoir ceux de l'identité civile et sans rechercher à retrouver la personne dans son contexte physique. Cette forme nouvelle d'identification, qu'on qualifiera d'innovante, repose sur une numérotation des acteurs de la communication. Ce numéro, par exemple contenu dans un cookie[28], permettra de reconnaître une personne déterminée, ou du moins sa machine, à l'occasion de ses navigations. Cette donnée identifiante permet de compiler l'information délivrée par l'internaute lors de navigations successives en vue de constituer des profils identitaires.

L'identification innovante recourt au marquage de l'internaute. Un marqueur électronique est apposé sur chaque internaute et permet de le resituer à l'intérieur de l'environnement électronique.

Ces nouveaux procédés d'identification méritent notre attention, car ils favorisent une forme nouvelle d'atteinte à la vie privée. Certes contenue à l'intérieur de l'environnement électronique, cette forme d'identification permet de suivre les agissements d'une personne sur le réseau. Cela offre la possibilité de dresser des profils précis, de la rejoindre électroniquement et d'adapter l'information communiquée en fonction du profil préétabli. À cela s'ajoute, la frontière ténue entre identification innovante et traditionnelle : la première pouvant à tout moment déboucher sur une identification d'une personne dans son contexte physique.

2. Les données identifiantes sur Internet[29]

1° L'adresse IP

La communication sur Internet s'appuie sur le protocole TCP/IP. La caractéristique de ce protocole est d'identifier tout ordinateur accédant au réseau à l'aide d'une adresse IP (pour *Internet Protocol*). Le concept même de communication suppose un adressage de l'information entre ordinateurs déterminés. L'adresse IP apparaît donc comme une donnée indispensable, à tout le moins pour déterminer le destinataire d'une information transmise sur le réseau. L'adresse IP est communiquée dans les différentes applications existant sur Internet : courrier électronique, consultation de sites Web.

Cette adresse s'apparente à un numéro de téléphone et désigne le lieu où s'est opérée l'entrée sur le réseau. Il faut noter que l'on rencontre sur

---

28 *Cf. infra.*

29 De précieuses indications peuvent être trouvées sur ce sujet particulièrement sensible dans les articles suivants : J.-M. DINANT, « Les traitements invisibles sur Internet », accessible à l'adresse http://www.droit.fundp.ac.be/crid/eclip/Luxembourg.html ; J.-M. DINANT, « L'électronisation du commerce », *La revue générale*, 1999, n° 3, pp. 39-47.

Internet deux formes d'adresses IP : les adresses IP permanentes et les adresses IP temporaires.

Les premières sont des adresses attribuées durablement à un ordinateur : tel est le cas des ordinateurs connectés au réseau *via* une université : l'université dispose en général d'un nombre d'adresses IP suffisant pour en attribuer une à chacun de ses utilisateurs. Les secondes sont des adresses attribuées à l'internaute pour la durée d'une seule connexion au réseau. C'est la situation actuelle auprès des fournisseurs d'accès commerciaux : disposant d'un nombre restreint d'adresses IP, ils attribuent au client une adresse IP temporaire, qui diffère à chacune de ses connexions.

Dans quelle mesure l'adresse IP constitue-t-elle une donnée identifiante ? Deux plans doivent être distingués : celui de l'identification traditionnelle (a) et celui de l'identification innovante (b)

a) La connaissance de l'adresse IP ne permet pas de retrouver automatiquement la personne physique utilisatrice. En effet, seul le fournisseur d'accès (université ou fournisseur commercial) peut indiquer à qui il a attribué telle ou telle adresse IP.

   À ce stade, s'ouvre un débat délicat, le fournisseur d'accès doit-il révéler l'identité civile qui se cache derrière telle adresse IP ? Sans pouvoir mener la réflexion à son terme, on constate d'emblée que deux approches s'opposent : Premièrement, le fournisseur doit-il communiquer les coordonnées d'une personne physique qu'il a conservées ? Sur ce point, la réponse devrait être positive lorsque cette communication a pour but « la sauvegarde d'un droit légalement reconnu ou judiciairement constaté »[30]. Deuxièmement, le fournisseur d'accès est-il autorisé à conserver les données reliant adresses IP et identité civile (en ce qui concerne les adresses IP temporaires, il s'agit de listings indiquant à qui telle adresse IP a été attribuée à tel moment déterminé) ? Sur ce point, l'affirmative n'est pas évidente : la conservation d'un fichier de correspondance entre adresses IP et identités civiles est un cas de traitement de données personnelles ; le principe de finalité s'applique. Si le fournisseur conserve de telles données à des fins de tarification, la finalité apparaît légitime. Mais une telle finalité tombe lorsque, et c'est souvent le cas, la tarification est forfaitaire.

   Il existe une deuxième possibilité d'identifier le titulaire d'une adresse IP. Elle consiste à établir la correspondance entre

30 Cass. fr., Civ. 1ère 6 novembre 1990, IR.278 cité par V. SÉDALLIAN, *Droit de l'Internet. Réglementation. Responsabilités. Contrats*, Paris, Ed. Net Press, pp. 242-244. L'auteur analyse en détail la question.

l'adresse IP utilisée et le numéro de téléphone au départ duquel a été établie la connexion matérielle au réseau.

b) En ce qui concerne l'identification innovante, on constatera que dans l'hypothèse d'une adresse IP permanente, il y a moyen de relier entre elles les différentes apparitions de cette adresse.

Cela dit, la recherche d'un point stable permettant de suivre dans la durée un utilisateur s'effectuera essentiellement grâce à la technique des cookies (*cf.* 4°)

2° Le nom de domaine

Le nom de domaine apparaît comme une traduction quelque peu conviviale de l'adresse IP. Il consiste en une suite de mots ou d'abréviations et permet de se faire une idée de l'identité d'un site.

Le système des noms de domaine a été mis en place au profit des serveurs Internet qui souhaitaient disposer d'une adresse qui soit plus parlante qu'une suite de chiffres[31]. La demande d'un nom de domaine est effectuée auprès d'un organisme de gestion des noms de domaine, lequel procède à une vérification de l'identité du demandeur.

Il est, en principe, possible d'obtenir auprès de ces organismes les coordonnées du responsable du site qui a demandé un nom de domaine. « L'identification du responsable d'un serveur d'information est donc très facile si un nom de domaine a été déposé »[32].

3° L'adresse de courrier électronique

En ce qui concerne l'auteur de messages, l'élément d'identifiabilité le plus visible consiste en son adresse de courrier électronique. Il s'agit de l'adresse utilisée pour désigner le destinataire et l'émetteur d'un message dans les applications de courriers électroniques et les groupes de discussion. Cette adresse comporte deux sortes de données, situées à gauche et à droite de l'arobace (symbole @). À gauche de l'@, figurent les données relatives à un utilisateur spécifique (une personne, une collectivité,…). À droite de l'arobace, figure le nom de domaine du fournisseur d'accès à Internet.

Sur le plan de l'identification innovante, l'adresse de courrier électronique apparaît comme l'outil par excellence pour suivre dans le temps une personne. Disposant de son adresse, tout internaute va pouvoir

---

31 L'interrogation sous la forme http://nomdedomaine ne va pas se diriger directement vers le serveur désigné. La requête va, tout d'abord, être traitée par un serveur spécifique, le serveur DNS, qui gère une liste d'équivalence entre les deux formes d'adresses et va assurer la traduction du nom de domaine en l'adresse IP correspondante.

32 V. SÉDALLIAN, *op. cit.*, p. 240.

lui attribuer la paternité de ses messages successifs et lui envoyer à son tour du courrier.

Sur le terrain de l'identification traditionnelle, la question qui se pose est de savoir si l'adresse de courrier électronique permet de retrouver l'individu qui est derrière l'adresse.

Deux cas de figure peuvent se présenter : dans le premier, l'adresse de courrier électronique contient des données identifiantes, par exemple un nom et un prénom. Pour peu que ces données s'avèrent exactes, on dispose, dès ce moment, d'un début d'information qui permettra éventuellement de retrouver cette personne (cela dit dans un contexte mondial, la connaissance d'éléments de l'état civil d'une personne ne garantit pas l'identification).

L'autre cas de figure concerne les adresses opaques, constituées de chiffres, de mots, qui ne livrent, à première lecture, aucune information sur l'identité de leur titulaire. Dans ce cas, seul le recours au fournisseur d'accès permet de retrouver l'internaute. Sur les modalités de diffusion de l'identité d'un de ses clients par le fournisseur d'accès, on se référera à ce qui a été dit précédemment à propos de la titularité des adresses IP[33]. En effet, l'adresse de courrier n'est qu'un équivalent convivial de l'adresse IP : elle offre une plus grande transparence et permet d'assurer le lien entre les adresses IP temporaires d'une même personne.

4° les cookies

Les cookies sont des informations persistantes enregistrées sur la machine du client Internet. Il s'agit pour le serveur de disposer d'un outil de reconnaissance d'un internaute, tantôt pour faciliter les navigations, tantôt pour recueillir des informations relatives à ce client. Ainsi l'internaute prête le flanc à la constitution, au fil de ses navigations au sein d'un même nom de domaine, d'un véritable profil dont le cookie constitue le socle.

Le cookie va donc apparaître comme l'outil par excellence en vue d'identifications innovantes. Il permet d'amalgamer les informations relatives à un même utilisateur lors de ses navigations au sein d'un même nom de domaine. Le caractère invisible des traitements opérés par les cookies et leur caractère incontournable (le cookie est fréquemment imposé comme condition d'accès à tel ou tel site) ont été dénoncés[34].

---

33 De manière générale, le fournisseur d'accès va être tenu d'une obligation de non-divulgation de l'identité et de l'adresse de ses clients. Cette obligation découlant du droit au respect de la vie privée va néanmoins céder le pas tant en présence d'infractions pénales, que pour assurer la sauvegarde d'un droit légalement reconnu ou judiciairement constaté.

34 J.-M. DINANT, « Les traitements invisibles sur Internet », accessible à l'adresse http://www.droit.fundp.ac.be/crid/eclip/Luxembourg.html

§ 2. L'anonymisation des communications sur Internet

Ayant conscience du polymorphisme des identifications sur Internet, il convient à ce stade de décrire les possibilités qui ont été imaginées pour couper court à ces identifications : on les désigne sous le terme de techniques d'anonymisation. Pour la clarté de notre exposé, il convient de distinguer deux applications distinctes qu'offre l'Internet : les applications de type courrier électronique, d'une part, et la consultation de sites web, d'autre part.

1. Envoi de messages (courrier électronique et groupes de discussion)

1° Recours à un réexpéditeur anonyme[35]

Lors de l'envoi d'un courrier électronique, l'élément d'identification le plus visible est, évidemment, l'adresse de courrier électronique[36]. Elle recouvre une donnée également accessible aux initiés : l'adresse IP de l'émetteur.

La technique la plus répandue d'anonymisation des messages consiste en leur réexpédition par un *anonymous remailer*. Ce réexpéditeur est un nouvel acteur du réseau. Sa tâche consiste à réceptionner un message émanant d'un internaute identifiable, pour ensuite le réexpédier à l'adresse du destinataire désigné, en ayant pris soin de supprimer toutes informations concernant l'émetteur du message et les sites par lesquels ce dernier a transité. Concrètement l'en-tête contenant l'adresse de courrier électronique sera effacée, de même que l'adresse IP de l'auteur du message.

2° Relativité des anonymisations

Il convient d'insister sur le caractère, par essence, relatif de l'anonymat. À l'instar du crime parfait, il faut constater que l'anonymat absolu est bien difficile à orchestrer.

Sur Internet, l'anonymisation opérée par les remailers peut déboucher soit sur un anonymat traçable, soit sur un anonymat intraçable. L'anonymat traçable vise l'hypothèse où le réexpéditeur détient les

---

35 Une recherche, *via* un moteur de recherche fournit une quantité importante d'information sur les *anonymous remailers* : pour exemple http://www.eff.org/pub/Net_info/Tools/Crypto/Anonymity/WWW_remailer/

36 Il convient de souligner l'opacité que peut présenter l'adresse de courrier électronique, opacité qui pourrait être levée auprès du fournisseur d'accès. A cela s'ajoute la possibilité, pour les initiés, de fabriquer de fausses adresses dotées celles-là d'une opacité durable. On omettrait d'évoquer un procédé simple d'envoi anonyme: sur le mode des cabines téléphoniques, il est possible d'accéder au réseau *via* des points d'accès collectifs (cybercafés, bornes situées dans les administrations publiques). Cela dit un contrôle des identités est fréquemment mis en place pour prévenir tout abus.

données relatives à l'identité de l'expéditeur du message. À ce stade, la clarification doit résider dans les conditions auxquelles ces réexpéditeurs pourraient être tenus de révéler l'identité de l'auteur d'un message. On peut estimer qu'au même titre que les fournisseurs d'accès, ils seraient tenus de préserver l'anonymat de leurs clients, mais que la révélation des identités pourrait être ordonnée dans l'hypothèse d'infractions ou d'abus.

La technique offre également des possibilités d'anonymat intraçable, et ce sous deux formes. Soit le réexpéditeur s'abstient de conserver l'information relative à l'identité de l'auteur ; il se met de la sorte dans l'impossibilité matérielle de révéler toute information sur l'identité de l'auteur. Soit l'auteur a recours à plusieurs remailers successifs et à la confidentialisation des contenus que permet la cryptographie à clé publique. L'objectif est d'empêcher toute traçabilité. Dans un tel système, le dernier remailer n'a pas connaissance de l'identité de celui qui a écrit le message qu'il réexpédie et personne n'est en mesure d'établir cette identité.

Dans l'hypothèse d'un anonymat intraçable, il faut souligner que l'intraçabilité reste une construction fragile ce qui conforte l'idée selon laquelle l'anonymat absolu est chose rare.

Ajoutons encore que l'anonymisation peut parfois prendre la forme d'une pseudonymisation : l'auteur dont l'identité n'est pas révélée se voit attribuer un pseudonyme qui permettra de le rejoindre via le réseau : ce pseudonyme fait office d'identité d'emprunt.

2. Consultation de sites Web

La consultation de sites web offre de nombreuses possibilités d'identification, soit au travers de l'adresse IP (identification traditionnelle ou innovante), soit au travers des cookies (identification innovante). Là encore, des entités vont offrir leurs services pour servir d'écran à l'internaute. L'accès aux différents sites se fera au travers de sites d'anonymisation, les serveurs proxy[37], qui préviendront la communication de toutes données identifiantes.

CONCLUSION

§1. Principe d'identifiabilité et anonymat d'exception

Un argument répandu en faveur de l'anonymat sur Internet consiste à dire qu'il est, dès à présent, la norme dans les comportements. Ainsi, il n'y

37 Un site de référence est certainement celui de l'anonymiser : http://www.anonymizer.com/3.0/index.shtml

pas lieu de décliner son identité à chacune des interactions de la vie en société. Cet argument confond anonymat et absence d'identification formelle. La personne, interviewée à visage découvert, cesse d'être anonyme. La communication d'une donnée identifiante, son apparence physique, la rend identifiable[38].

La mise en évidence d'un principe général d'identifiabilité est un jalon de première importance dans le débat en cours. L'anonymat actif ne peut voir le jour qu'à titre d'exception à ce principe général. Il doit répondre à une finalité précise justifiant l'exception. Ainsi, l'anonymat est parfois admis sur les plateaux de télévision : un orateur masqué, à la voix déformée, est interviewé. La finalité est ici de protéger la sphère d'intimité de cette personne. Le procédé reste exceptionnel et n'est utilisé qu'en cas de risques réels.

Les moyens à mettre en œuvre pour échapper aux identifications sont, quant à eux, lourds. Ceci est d'autant plus vrai dans le contexte actuel, où les techniques d'identification sont des plus performantes.

§2. Anonymat d'expression et de protection

Deux formes d'anonymat retiennent particulièrement l'attention. Elles poursuivent deux finalités spécifiques : l'exercice de la liberté d'expression et la protection de sa vie privée. Sur ces terrains, l'identification est vécue comme dommageable.

Tout d'abord, elle bride l'expression. La reconnaissance par la Cour suprême des États-Unis d'un véritable droit à l'anonymat pour assurer le respect du premier amendement est de première importance. L'anonymat est reconnu comme une modalité nécessaire de la liberté d'expression. Il vient renforcer la substance même de la communication ; l'expression anonyme permet d'exprimer des opinions nouvelles, d'enrichir le débat sur les idées.

Toute la difficulté consiste à trouver un équilibre entre la préservation, dans le cadre de la liberté d'expression, de *l'obligation de rendre compte*, appuyée par le principe d'identifiabilité, et ce droit à l'expression anonyme. Consciente de cette difficulté, la jurisprudence américaine donne une portée étroite au droit à l'anonymat. Pour le reste, il faut considérer que la valeur à protéger justifie que la mise en œuvre de *l'obligation de rendre compte* soit, dans une certaine mesure, entravée.

Sur le terrain de la vie privée, l'anonymisation est recherchée car les identifications successives qu'implique la vie en société représentent une menace croissante pour l'individu. C'est la logique d'identification poussée à l'extrême qui provoque la recherche d'un tel moyen de défense.

38 C'est d'ailleurs cette identifiabilité qui fonde le droit à l'image.

Jusqu'alors les nombreuses identifications passives n'étaient pas recoupées entre elles, ni conservées durablement. Le principe d'identifiabilité se vivait de manière segmentée. Le phénomène d'identification en continu permet, quant à lui, la traçabilité de l'homme moderne.

Dans les deux cas, la revendication de l'anonymat émane de l'individu. En cela, il y a distinction avec les cas d'anonymats circonstanciels mis en place par l'autorité. Le mouvement amorcé semble indiquer que l'individu souhaite exercer une maîtrise accrue sur ses données identifiantes. Nous l'évoquerons au titre de l'autonomie identitaire.

§3. Techniques identifiantes

L'anonymat sur Internet s'inscrit dans un environnement technique. La première donnée observée est l'abondance des identifications opérées sur le réseau. Il faut cependant différencier les identifications requises entre ordinateurs et l'identification des utilisateurs de ces machines. La clé des premières est l'adresse IP. C'est grâce à cet élément d'identification qu'un ordinateur accède au réseau, y diffuse ou en retire de l'information. Cela dit le bon fonctionnement du réseau n'impose pas la connaissance de l'identité civile de chaque intervenant. Il convient de clarifier les conditions dans lesquelles les données nécessaires aux identifications techniques peuvent conduire à une identification traditionnelle. Il s'agit, en particulier, de préciser les obligations des fournisseurs d'accès et des *anonymous remailers* : conditions de conservation des tables de correspondance entre adresse IP et identité civile des utilisateurs dans le chef des fournisseurs d'accès, condition de fourniture d'un service d'anonymisation, conditions de divulgation d'une identité civile.

Le recours aux cookies doit également être clarifié. Les identifications innovantes qu'il entraîne apparaissent à première vue anodines. Elles représentent un premier danger en ce qu'elles permettent l'accumulation de tous les faits et gestes accomplis par un internaute sur tel ou tel site. Il est urgent de pouvoir mesurer les conséquences que peut avoir ce type de compilations d'informations. Le deuxième danger tient au fait que la frontière entre identification innovante et identification traditionnelle est ténue. En recoupant tel profil identitaire avec des données relatives à des ventes par correspondance, il devient aisé de pouvoir mettre un nom et un visage sur ce qui, au départ, n'était qu'un simple profil.

Au-delà des données techniques, il faut constater que les réponses posées sur le terrain des identifications appellent des réponses juridiques.

§4. L'autonomie identitaire

Le souhait d'anonymat exprimé par de nombreux internautes apparaît, essentiellement, comme une réaction à l'efflorescence des identifications. Cette dernière accompagne les différentes avancées technologiques en matière de communication : les nouveaux réseaux téléphoniques indiquent instantanément le numéro de communication de l'appelant ; les réseaux de téléphonie mobile conservent la trace de tous les déplacements, les réseaux bancaires celle des achats et retraits d'argent. Et, cet article en témoigne, Internet n'est pas en reste.

L'anonymat est souvent présenté comme une menace car il paralyserait les identifications. Il nous semble qu'il faille renverser les termes de ce débat. C'est la légitimité des identifications qui doit être étudiée. Dans l'immédiat, l'anonymat n'est qu'une réponse logique et fragile à l'augmentation de ces dernières.

Le principe général d'identifiabilité semble, aujourd'hui, mis à mal par les identifications massives et leur portée sans cesse élargie. Ce principe résulte d'un compromis ancien sur le terrain de l'identité ; les identifications qu'il entraîne ont été acceptées par l'individu, le groupe et l'autorité. La revendication individuelle à l'anonymat semble vouloir dire que l'individu conteste, désormais, la façon dont est appliqué le principe. La multiplication quantitative et qualitative des identifications au profit de l'autorité ou du groupe porte atteinte à l'autonomie de l'individu sur ses données identitaires.

Il nous semble qu'il faut dépasser le débat actuel qui oppose révélation et dissimulation de l'identité. Il convient d'entreprendre un débat beaucoup plus nuancé qui porterait sur l'autonomie identitaire reconnue à l'individu et qui viserait la maîtrise de l'individu sur ses données identifiantes. Cette autonomie vise à la fois la communication des données identifiantes et la maîtrise de l'usage qui en sera fait ultérieurement. Il est clair que les identifications invisibles, ainsi que les identifications dont on ne perçoit pas les finalités portent directement atteinte à cette autonomie.

Entre anonymat et révélation de l'identité, il existe d'autres modalités d'interactions. À ce titre, les intermédiaires à la communication sont appelés à jouer un rôle important afin de minimiser les intrusions sur le terrain de l'identité, tout en assurant le respect de *l'obligation de rendre compte*.